

SECURITY SUPPORT SERVICES STATEMENT OF WORK ADDENDUM

NIWC PACIFIC WORK WEEK

(a) All or a portion of the effort under this contract will be performed on a Government installation. The normal workweek for Government employees at NIWC Pacific is Monday through Thursday 7:15AM to 4:45PM and Friday 7:15AM to 3:45PM with every other Friday a non-work Friday. Work at this Government installation, shall be performed by the contractor within the normal workweek unless differing hours are specified on the individual task orders. Following is a list of holidays observed by the Government:

<u>Name of Holiday</u>	<u>Time of Observance</u>
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Juneteenth National Independence Day	19 June
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the Contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the Contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations, the payment of overtime is required only when an employee works more than 40 hours during a week. Therefore, during the NIWC Pacific off-Friday (36-hour) week overtime will not be paid for non-exempt employees. During the work-Friday week (44 hour) the contractor is to schedule work so as not to incur overtime charges during the normal work week unless authorized in writing by the Government to do so. An example of this would be for contractor personnel to work during the hours of 7:15 AM to 4:45 PM Monday through Thursday and 7:15 AM to 3:45 PM Friday during the work-Friday week. The contractor may also elect to configure the workforce in such a way that no single employee exceeds 40 hours during a normal week even though normal NIWC Pacific hours are maintained both weeks.

(e) NOTICE: All Contractor employees who make repeated deliveries to military installations shall obtain the required employee pass via the Navy Commercial Access Control System (NCACS) in order to gain access to the facility. Information about NCACS may be found at the following website: <http://www.rapidgate.com/>.

Contractor employees must be able to obtain a NCACS in accordance with base security requirements. Each employee shall wear the Government issued NCACS badge over the front of the outer clothing. When an employee leaves the Contractor's employ, the employee's NCACS pass shall be returned to the Contracting Officer's Representative or the base Badge and Pass Office within five (5) calendar days.

Contractors who do not have a NCACS or Common Access Card (CAC) must be issued a one-day pass daily at the Badge and Pass Office. Issuance of a CAC requires the need for physical access to the installation and logical access to government owned computer systems.

(f) Periodically the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises which may require the Contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The Contractor will be required to work with its Government point of contact to adjust

work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours, or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

LIABILITY INSURANCE – COST TYPE CONTRACTS

(a) The following types of insurance are required in accordance with FAR 52.228-7 “Insurance--Liability to Third Persons” and shall be maintained in the minimum amounts shown:

- (1) Workers’ compensation and employers’ liability: minimum of \$100,000
- (2) Comprehensive general liability: \$500,000 per occurrence
- (3) Automobile liability: \$200,000 per person
\$500,000 per occurrence
\$ 20,000 per occurrence for property damage

(b) When requested by the contracting officer, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

CONTRACTOR IDENTIFICATION

(a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.

(c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with contractor supplied signs, name plates or other identification, showing that these are work areas for contractor or subcontractor personnel.

REIMBURSEMENT OF TRAVEL COST – ALTERNATE II

(a) Contractor Request and Government Approval of Travel

Any travel under this contract must be specifically requested in writing, by the contractor prior to incurring any travel costs. If this contract is an indefinite-delivery contract, then the written Government authorization will be by task/delivery orders issued by the Ordering Officer or by a modification to an issued task/delivery order. If this contract is an indefinite-delivery contract, then the written Government authorization will be by written notice of approval from the Contracting Officer’s Representative (COR). The request shall, at a minimum, include:

- (1) Contract number
- (2) Date, time, and place of proposed travel
- (3) Purpose of travel and how it relates to the contract
- (4) Contractor’s estimated cost of travel
- (5) Name(s) of individual(s) traveling and;
- (6) A breakdown of estimated travel and per diem charges.

The contractor shall submit the travel request in writing to the Contracting Officer’s Representative (COR). The COR shall review and approve/disapprove (as appropriate) all travel requests submitted giving written notice of such approval or disapproval to the contractor.

(b) General

(1) The costs for travel, subsistence, and lodging shall be reimbursed to the contractor only to the extent that it is necessary and authorized for performance of the work under this contract. The costs for travel, subsistence, and lodging shall be reimbursed to the contractor in accordance with the Federal Acquisition Regulation (FAR) 31.205-46, which is incorporated by reference into this contract. As specified in FAR 31.205-46(a) (2), reimbursement for the costs incurred for lodging, meals and incidental expenses (as defined in the travel regulations cited subparagraphs (b)(1)(i) through (b)(1)(iii) below) shall be considered to be reasonable and allowable only to the extent that they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel as set forth in the following:

(i) Federal Travel Regulation prescribed by the General Services Administration for travel in the contiguous 48 United States;

(ii) Joint Travel Regulation, Volume 2, DoD Civilian Personnel, Appendix A, prescribed by the Department of Defense for travel in Alaska, Hawaii, The Commonwealth of Puerto Rico, and the territories and possessions of the United States; or

(iii) Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in the travel regulations cited in subparagraphs (b)(1)(i) and (b)(1)(ii) above.

(2) Personnel in travel status from and to the contractor's place of business and designated work site or vice versa, shall be considered to be performing work under the contract, and contractor shall bill such travel time at the straight (regular) time rate; however, such billing shall not exceed eight hours per person for any one person while in travel status during one calendar day.

(c) Per Diem

(1) The contractor shall not be paid per diem for contractor personnel who reside in the metropolitan area in which the tasks are being performed. Per diem shall not be paid on services performed at contractor's home facility and at any facility required by the contract, or at any location within a radius of 50 miles from the contractor's home facility and any facility required by this contract.

(2) Costs for subsistence and lodging shall be paid to the contractor only to the extent that overnight stay is necessary and authorized in writing by the Government for performance of the work under this contract per paragraph (a). When authorized, per diem shall be paid by the contractor to its employees at a rate not to exceed the rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and authorized in writing by the Government. The authorized per diem rate shall be the same as the prevailing locality per diem rate.

(3) Reimbursement to the contractor for per diem shall be limited to payments to employees not to exceed the authorized per diem and as authorized in writing by the Government per paragraph (a). Fractional parts of a day shall be payable on a prorated basis for purposes of billing for per diem charges attributed to subsistence on days of travel. The departure day from the Permanent Duty Station (PDS) and return day to the PDS shall be 75% of the applicable per diem rate. The contractor shall retain supporting documentation for per diem paid to employees as evidence of actual payments.

(d) Transportation

(1) The contractor shall be paid on the basis of actual amounts paid to the extent that such transportation is necessary for the performance of work under the contract and is authorized in writing by the Government per paragraph (a).

(2) The contractor agrees, in the performance of necessary travel, to use the lowest cost mode commensurate with the requirements of the mission and in accordance with good traffic management principles. When it is necessary to use air or rail travel, the contractor agrees to use coach, tourist class or similar accommodations to the extent consistent with the successful and economical accomplishment of the mission for which the travel is being

performed. Documentation must be provided to substantiate non-availability of coach or tourist if business or first class is proposed to accomplish travel requirements.

(3) When transportation by privately owned conveyance (POC) is authorized, the contractor shall be paid on a mileage basis not to exceed the applicable Government transportation rate specified in the travel regulations cited in FAR 31.205-46(a)(2) and is authorized in writing by the Government per paragraph (a).

(4) When transportation by privately owned (motor) vehicle (POV) is authorized, required travel of contractor personnel, that is not commuting travel, may be paid to the extent that it exceeds the normal commuting mileage of such employee. When an employee's POV is used for travel between an employee's residence or the Permanent Duty Station and one or more alternate work sites within the local area, the employee shall be paid mileage for the distance that exceeds the employee's commuting distance.

(5) When transportation by a rental automobile, other special conveyance or public conveyance is authorized, the contractor shall be paid the rental and/or hiring charge and operating expenses incurred on official business (if not included in the rental or hiring charge). When the operating expenses are included in the rental or hiring charge, there should be a record of those expenses available to submit with the receipt. Examples of such operating expenses include hiring charge (bus, streetcar or subway fares), gasoline and oil, parking, and tunnel tolls.

(6) Definitions:

(i) "Permanent Duty Station" (PDS) is the location of the employee's permanent work assignment (i.e., the building or other place where the employee regularly reports for work.

(ii) "Privately Owned Conveyance" (POC) is any transportation mode used for the movement of persons from place to place, other than a Government conveyance or common carrier, including a conveyance loaned for a charge to, or rented at personal expense by, an employee for transportation while on travel when such rental conveyance has not been authorized/approved as a Special Conveyance.

(iii) "Privately Owned (Motor) Vehicle (POV)" is any motor vehicle (including an automobile, light truck, van or pickup truck) owned by, or on a long-term lease (12 or more months) to, an employee or that employee's dependent for the primary purpose of providing personal transportation, that:

- (a) is self-propelled and licensed to travel on the public highways;
- (b) is designed to carry passengers or goods; and
- (c) has four or more wheels or is a motorcycle or moped.

(iv) "Special Conveyance" is commercially rented or hired vehicles other than a POC and other than those owned or under contract to an agency.

(v) "Public Conveyance" is local public transportation (e.g., bus, streetcar, subway, etc.) or taxicab.

(iv) "Residence" is the fixed or permanent domicile of a person that can be reasonably justified as a bona fide residence.

EXAMPLE 1: Employee's one way commuting distance to regular place of work is 7 miles. Employee drives from residence to an alternate work site, a distance of 18 miles. Upon completion of work, employee returns to residence, a distance of 18 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (14 miles). The employee is reimbursed for 22 miles ($18 + 18 - 14 = 22$).

EXAMPLE 2: Employee's one way commuting distance to regular place of work is 15 miles. Employee drives from residence to an alternate work site, a distance of 5 miles. Upon completion of work, employee returns to residence, a distance of 5 miles.

In this case, the employee is not entitled to be reimbursed for the travel performed (10 miles), since the distance traveled is less than the commuting distance (30 miles) to the regular place of work.

EXAMPLE 3: Employee's one way commuting distance to regular place of work is 15 miles. Employee drives to regular place of work. Employee is required to travel to an alternate work site, a distance of 30 miles. Upon completion of work, employee returns to residence, a distance of 15 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (30 miles). The employee is reimbursed for 30 miles ($15 + 30 + 15 - 30 = 30$).

EXAMPLE 4: Employee's one way commuting distance to regular place of work is 12 miles. In the morning, the employee drives to an alternate work site (45 miles). In the afternoon, the employee returns to the regular place of work (67 miles). After completion of work, employee returns to residence, a distance of 12 miles.

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal round trip commuting distance (24 miles). The employee is reimbursed for 100 miles ($45 + 67 + 12 - 24 = 100$).

EXAMPLE 5: Employee's one way commuting distance to regular place of work is 35 miles. Employee drives to the regular place of work (35 miles). Later, the employee drives to alternate work site #1 (50 miles) and then to alternate work site #2 (25 miles). Employee then drives to residence (10 miles).

In this case, the employee is entitled to be reimbursed for the distance that exceeds the normal commuting distance (70 miles). The employee is reimbursed for 50 miles ($35 + 50 + 25 + 10 - 70 = 50$).

EXAMPLE 6: Employee's one way commuting distance to regular place of work is 20 miles. Employee drives to the regular place of work (20 miles). Later, the employee drives to alternate work site #1 (10 miles) and then to alternate work site #2 (5 miles). Employee then drives to residence (2 miles).

In this case, the employee is not entitled to be reimbursed for the travel performed (37 miles), since the distance traveled is less than the commuting distance (40 miles) to the regular place of work.

REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION

(a) Definition. As used in this text, "sensitive information" includes:

- (i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
- (ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);
- (iii) Information properly marked as "business confidential," "proprietary," "procurement sensitive," "source selection sensitive," or other similar markings;
- (iv) Other information designated as sensitive by the Naval Information Warfare Systems Command (NAVWAR).

(b) In the performance of the contract, the contractor may receive or have access to information, including information in Government information systems and secure websites. Accessed information may include "sensitive information" or other information not previously made available to the public that would be competitively useful on current or future related procurements.

(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The contractor shall—

- (i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;

- (ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;
- (iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contract and to safeguard information from unauthorized use and disclosure.
- (iv) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment;
- (v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the contractor may not be authorized to access such information, the contractor shall (i) notify the Contracting Officer; and (ii) refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this text are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government information systems.

(f) Subcontracts. The contractor shall insert paragraphs (a) through (f) of this text in all subcontracts that may require access to sensitive information in the performance of the contract.

(g) Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate contractor personnel requiring access to information in the performance of the contract from other contractor personnel to ensure that the contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE

The Contracting Officer hereby appoints the following individual as Contracting Officer's Representative (COR) for this contract/order:

Name: TBD

Code: TBD

Phone Number: TBD

E-mail: TBD

OFFSHORE PROCUREMENT OF COMSEC EQUIPMENT

Due to the sensitivity of Communications Security (COMSEC) and to maintain rigid control over the integrity of COMSEC equipment, no subcontracts or purchase orders which involve design, manufacture, production, assembly

or test in a location not in the United States, of equipment, assemblies, accessories or parts performing cryptographic functions shall be made under this contract without prior specific approval of the Contracting Officer. The contractor further agrees to include this text in all subcontracts it may issue pursuant to this contract for equipment, assemblies, accessories or parts.

CYBERSECURITY

Cybersecurity (which replaced the term Information Assurance (IA)) is defined as prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Contractor personnel shall perform tasks to ensure Navy applications, systems, and networks satisfy Federal/DoD/DON/Navy cybersecurity requirements.

Cyber IT and Cybersecurity Personnel

(a) The Cyberspace workforce elements addressed include contractors performing functions in designated Cyber IT positions and Cybersecurity positions. In accordance with DFARS Subpart 239.71, DoDD 8140.01, SECNAVINST 5239.20A, and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems. Proposed contractor Cyber IT and cybersecurity personnel shall be appropriately qualified prior to the start of the contract performance period or before assignment to the contract during the course of the performance period.

(b) The contractor shall be responsible for identifying, tracking and reporting cybersecurity personnel, also known as Cybersecurity Workforce (CSWF) and Cyber IT workforce personnel. Although the minimum frequency of reporting is monthly, the task order can require additional updates at any time.

(c) Contractors that access Navy IT shall also follow guidelines and provisions documented in Navy Telecommunications Directive (NTD 10-11) and are required to complete a System Authorization Access Request (SAAR) – Navy form as documented in para 8.2.2.4(b).

When a contractor requires logical access to a government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official government issued e-mail address (e.g., .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the NIWC Pacific Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: <https://twms.nmci.navy.mil/>. For those contractors requiring initial training and do not have a CAC, contact the NIWC Pacific IAM office. Training can be taken at the IAM office or online at <http://iase.disa.mil/index2.html>.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the NIWC Pacific IAM office or from the website: <https://navalforms.documentservices.dla.mil/>.

(d) Contractor personnel with privileged access will be required to acknowledge special responsibilities with a Privileged Access Agreement (PAA) IAW SECNAVINST 5239.20A.

Design, Integration, Configuration or Installation of Hardware and Software

The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01. The contractor shall ensure that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/Authorization official. Contractors that access Navy IT are also required to follow the provisions contained in DON CIO Memorandum:

Acceptable Use of Department of the Navy Information Technology (IT) dated 12 Feb 16. Use of blacklisted software is specifically prohibited and only software that is registered in DON Application and Database Management System (DADMS) and is Functional Area Manager (FAM) approved can be used as documented in

para 5.2.2. Procurement and installation of software governed by DON Enterprise License Agreements (ELAs) – Microsoft, Oracle, Cisco, Axway, Symantec, ActivIdentity, VMware, Red Hat, NetApp, and EMC shall be in accordance with DON CIO Policy and DON ELAs awarded.

Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFARS PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report as applicable at the task order level. IAW DFARS clause 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided at the task order level, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other government representative the proper labor category cybersecurity designation and certification requirements.

Information Technology (IT) Services Requirements

This paragraph only applies to IT contracts. Information Technology (IT) is defined as any equipment or interconnected system(s) or subsystem(s) of equipment that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data of information by the agency. IT includes computers, ancillary equipment, peripherals, input, output, and storage devices necessary for security and surveillance. Electronic and Information technology (EIT) is IT that is used in the creation, conversion, or duplication of data or information. EIT includes: telecommunication products, such as telephones; information kiosks; transaction machines; World Wide Web sites; multimedia (including videotapes); and office equipment, such as copiers and fax machines.

Information Technology (IT) General Requirements

When applicable, the contractor shall be responsible for the following:

- Ensure that no production systems are operational on any RDT&E network.
- Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.
- Migrate all Navy Ashore production systems to the NMCI environment where available.
- Work with government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).
- Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.
- Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.
- Only perform work specified within the limitations of the task order.

Acquisition of Commercial Software Products, hardware, and Related Services

This paragraph only applies to the purchasing/hosting of commercial software. Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

DON Enterprise Licensing Agreement/DOD Enterprise Software Initiative Program

Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dated 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an

item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and government-wide SmartBuy program (see DoD memo dated 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the task order level.

DoN Application and Database Management System

The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

Section 508 Compliance

This paragraph only applies to IT contracts. The contractor shall ensure that all software recommended, procured, and/or developed is compliant with Section 508 of the Rehabilitation Act of 1973, 26 CFR Part 1194 and pursuant to SPAWARINST 5721.1B of 17 Nov 2009. In accordance with FAR 39.204, this requirement does not apply to contractor acquired software that is incidental to the task, software procured/developed to support a program or system designated as a National Security System (NSS) or if the product is located in spaces frequented only by service personnel for maintenance, repair or occasional monitoring of equipment.

Software Development/Modernization and Hosting

This paragraph only applies to software development and modernization. The contractor shall ensure all programs utilizing this contract for software development/ modernization (DEV/MOD), including the development of IT tools to automate NIWC Pacific business processes are compliant with DON Information Management/Information Technology (DON IM/IT) Investment Review Process Guidance requirements. Contractors shall neither host nor develop IT tools to automate NIWC Pacific business processes unless specifically tasked within the task order or contract. The contractor shall ensure IT tools developed to automate NIWC Pacific business processes will be delivered with full documentation and source code, as specified at the task order level, to allow non-proprietary operation and maintenance by any source. The contractor shall ensure all programs are submitted with proof of completed DEV/MOD certification approval from the appropriate authority in accordance with DON policy prior to task order award. *Note must be listed on Investment Review Board (IRB) approved list.

Information Security

Pursuant to DoDM 5200.01 and DoD 5200.48, the contractor shall provide adequate security for all CUI and unclassified DoD information passing through non-DoD information systems, including all subcontractor information systems utilized on contract. If the contractor originates, adds, or changes any of the DoD information, it must be marked in accordance with DODI 5200.48 and handled properly. The contractor shall disseminate CUI and unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

IT Position Designations

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of Special-Sensitive (SS)/Critical-Sensitive (CS) or Noncritical Sensitive (NCS), access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Per SECNAVINST 5510.30C, page 7, Section 8.b of enclosure (4), the Information Systems Security Manager is responsible for establishing, implementing and maintaining the DoN information

system and information assurance program and is responsible to the Commanding Officer for developing, maintaining, and directing the implementation of the Information Assurance (IA) program within the command. The three basic position sensitivity levels/Position Designations:

- Special-Sensitive (SS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for inestimable impact and/or damage.
- Critical-Sensitive (CS)/T5 or T5R; equivalent (SSBI, etc.) (IT Level I) - Potential for grave to exceptionally grave impact and/or damage.
- Noncritical Sensitive (NCS)/T3 or T3R; equivalent (ANAC/ANACI) (IT Level II) - Potential for some to serious impact and/or damage.

CONTRACTOR NOTIFICATION – AWARENESS OF EXPECTATIONS

Contractor personnel must adhere to all current DoD, SECNAV, OPNAV, and NIWC Pacific instructions related to foreign travel.

Contractor personnel are reminded of their obligation to safeguard the vital relationship our Nation has with Foreign Countries. This includes personal conduct while performing under the contract and on one's personal time because, at all times, you are viewed by our partners as a representative of the United States, our Navy, and NAVWAR. Therefore, professional, courteous, and culturally aware conduct is necessary at all times. Inappropriate conduct, and especially intoxication and criminal behaviors, will not be tolerated. An all too common nexus for personnel misconduct while on travel is irresponsible consumption of alcohol. Intoxication increases your vulnerability to crime, injury, arrest, terrorism and espionage.

While traveling on official business, representing and performing in support of NAVWAR's mission, all personnel, including military, civilian and contractors, are expected to act in a professional and responsible manner. In order to promote effective relationships with business partners and allied nations, it is incumbent on contractor personnel to follow local laws and employ courteous and culturally aware behavior. Inappropriate conduct may jeopardize important relationships for the United States Navy, NAVWAR, NIWC Pacific and NIWC Atlantic, and will not be tolerated.

In all cases, contractors are reminded of their responsibilities under FAR Subpart 3.10, Contractor Code of Business Ethics and Conduct, and specifically FAR 3.1002, which requires contractors to conduct themselves with the highest degree of integrity and honesty.

Additionally, in accordance with FAR 3.1003(a)(2), contractors may be suspended and/or debarred for failing to timely disclose to the Government, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, credible evidence that a principal, employee, agent, or subcontractor of the contractor has committed—

- A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or
- A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

INTELLIGENCE OVERSIGHT

In compliance with DoDD 5148.13 paragraph 4.1.e and SECNAVINST 3820.3F, for any contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA), Significant, or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

Questionable Intelligence Activity (QIA): Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

Significant or Highly Sensitive Matter (S/HSM): An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

- Congressional inquiries or investigations
- Adverse media coverage
- Impact on foreign relations or foreign partners
- Systemic compromise, loss, or unauthorized disclosure of protected information.